UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/017,739	12/18/2001	Michael D. Ladwig	3351-029A (PRC-127)	9729

7590 06/29/2004

LOWE HAUPTMAN GILMAN & BERNER, LLP
Suite 310
1700 Diagonal Road
Alexandria, VA 22314

EXAMINER	
BONZO, BRYCE P	
ART UNIT	PAPER NUMBER
2114	16

DATE MAILED: 06/29/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES PATENT AND TRADEMARK OFFICE

COMMISSIONER FOR PATENTS
UNITED STATES PATENT AND TRADEMARK OFFICE
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/017,739
Filing Date: December 18, 2001
Appellant(s): LADWIG, MICHAEL D.

Kenneth M Berner
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed April 27th, 2004.

(1) Real Party in Interest

A statement identifying the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

A statement identifying the related appeals and interferences which will directly affect or be directly affected by or have a bearing on the decision in the pending appeal is contained in the brief.

(3) Status of Claims

The statement of the status of the claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Invention

The summary of invention contained in the brief is correct.

(6) Issues

The appellant's statement of the issues in the brief is correct.

(7) Grouping of Claims

Appellant's brief includes a statement that claims 1, 2, 4-6, 16, 22, 24 and 26 do not stand or fall together and provides reasons as set forth in 37 CFR 1.192(c)(7) and (c)(8).

(8) Claims Appealed

The copy of the appealed claims contained in the Appendix to the brief is correct.

(9) Prior Art of Record

5,787,253	McCreery et al.	9-1998

(10) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Rejections under 35 USC §102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1, 4-6, 8, 15-19, 22, 24, 26, 28, 31 and 32 are rejected under 35 U.S.C. 102(e) as being anticipated by McCreery.

As per claim 1, McCreery discloses:

A method for monitoring a computer network for specified events at a presence, comprising (Abstract):

gathering heterogeneous data (column 4, lines 48-63: "*many different nodes may be captured*" describes one manner in which to interpret *heterogeneous*; column 5, lines 1-10: while *FTP, HTTP, SMTP, TELNET* describe other ways to interpret heterogeneous data),

as directed by the presence (column 4, lines 5-56:describe an entity directing and analyzing the monitoring system; column 4, lines 45-47: describe a packet filtering system which inside a greater entity which is in charge of the monitoring system and some undisclosed system to configure this filter),

at two or more remote computers (column 4, lines 8-18: describes multiple networks, which must have multiple computes; column 4, lines 48-49: describe many nodes- specifically 5)

placing the gathered data in a data stream and forwarding the data stream to the presence (column 4, lines 63-65: the packet analysis system is the presence);

receiving, at the presence, the at least one data stream sent from two or more remote computers, the data steam including data representative of events (column 4, lines 41-43: "collect all raw packets" by definition will provide data representative of the network; column 4, lines 58-67: describe that the data is in fact received at the presence and not elsewhere); and

applying rules to the at least one data stream at the presence for sorting data representative (column 4, lines 44-57: describe applying rules, taking an action on a certain event is loosely defined as filtering the events in the buffer)

and for taking one or more actions based on a specific event (column 5, lines 44-57: describe clearly taking action specifically based on the output of the analysis system 270).

As per claim 4, McCreery discloses: wherein said gathering step is performed by an agent (column 4, lines 35-63 the network interface is an agent as it works on behalf of the analyzer).

As per claim 5, McCreery discloses: hunting for predetermined data at a remote location and placing the hunted data in a data stream and forwarding the data stream to the computer (the IP addresses of packets filtered by McCreery contain data stored at a remote location).

As per claim 6, McCreery discloses: the hunting is carried out by agents (column 4, lines 35-63 the network interface is an agent as it works on behalf of the analyzer).

As per claim 8, McCreery discloses: wherein the at least one data stream includes message traffic (column 2, lines 11-20).

As per claim 15, McCreery discloses: wherein an event is comprised of at least one of the following elements: types, title, *datetime*, keywords, summary priority and duration (Figure 5b-1).

As per claim 16, McCreery discloses: wherein a rule includes a criteria component and an action component (column 5, lines 47-57: Action-"notification", Criteria: "exceeds predetermined thresholds").

As per claim 17, McCreery discloses: wherein the criteria component includes at least one criteria statement and to satisfy a rule either all, any or none of the at least one criteria statements need to be satisfied. As McCreery shows, once the network exceeds a threshold (satisfies a rule criteria) action is takes (column 5, lines 52-57).

As per claim 18, McCreery discloses: at least one action is taken if the at least one rule is satisfied (column 5, lines 43-57).

As per claim 19, McCreery discloses: wherein the data in the event data stream is received in a standardized format (Figure 5c, Ethernet format).

Claim 22 is rejected in the manner of claim 1, as claim 22 is the article of manufacture embodiment of the method claim 1.

Claim 24 is rejected in the manner of claim 1, as claim 24 is the computer architecture embodiment of method claim 1.

Claim 26 is rejected in the manner of claim 1, as claim 26 is the computer system embodiment of method claim 1.

As per claim 28, McCreery discloses:

wherein said gathering step includes collecting/gathering data at two or more remote computes (column 6, lines 41-46).

As per claim 31, McCreery discloses:

wherein the action is automatically brought to the attention of the user (column 5, line 51).

As per claim 32, McCreery discloses:

wherein alert including one of an alert window, flashing icon, email and beeper notification is used automatically (column 7, lines 1-6).

Rejections under 35 USC §103(a)

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 2, 14, 20, 23, 27 and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over McCreery.

As per dependant claim 2, McCreery does not explicitly teach displaying the events in a timeline. McCreery does disclose the gathering and formatting of the information required to generate a timeline. Further, McCreery does specifically discloses the data is used to generate charts and graphs. Additionally, McCreery teaches the display of data in chronological order (Figures 5 and 7). A timeline provides easy user access to information in chronological order. Thus it would have been obvious to one of ordinary skill in the art at the time of invention to use the gathered information of McCreery to display a timeline.

As per claim 14, McCreery does not explicitly disclose: filing (storing) the sorted information in separate data stream files. McCreery does store data which has been modified and raw data, however does state that the data is stored separately. Given the purpose of creating the modified data is to "avoid redundant storage of the same data" (column 5, lines 30-35). Therefore it is clear McCreery is storing multiple sets of data. Thus it would have been obvious to one of ordinary skill in the art at the time of invention to store the sorted information separately from other information thus allowing easy access to the filtered information.

As per claim 20, McCreery discloses: displaying an event stream using information stored in stored stream files (column 5, lines 31-43, Figures 5).

Claim 23 is rejected in the manner of claim 2, as claim 23 is the article embodiment of the method claim 2.

Claim 27 is rejected in the manner of claim 2, as claim 27 is the computer system embodiment of method claim 2.

As per claim 29, McCreery discloses:

wherein said gathering and receiving step are preformed in real-time. McCreery discloses the use of a hardware device (that is a network device in promiscuous mode) taking data off of a network. As the network device is operating at a high speed and immediately processing the network data as soon as it is placed on the network, it is a real-time system.

(11) Response to Arguments

As per claim 1:

Applicant has asserted that McCreery does not "intercept" heterogeneous data. The packet analysis section is clearly receiving buffered data packets (column 4, lines 63-67) The fact that the packet analysis section receives and holds on to the packets meets the "gathering" requirement of the claim.

The second limitation allegedly not taught, is "intercepting." The packets which are fed to the packet analyzer originate on the network. McCreery clearly discloses the packets are not originally destined to the packet analyzer system, but are to be transmitted between five other nodes (column 5, lies 48-63). This satisfies the requirements for "intercepting".

The third limitation Applicant has asserted to not be taught is "applying rules to the at least one data stream at the presence for sorting data representative and for taking one or more actions based on a specific event." McCreery clearly describes filtering at column 4, lines 53-56. Filtering is the process of applying rules to refine data down to data which is of interest. McCreery discloses raising alarms in the system based on the results of the filtered data at column 5, lines 47-52. The raising of an alarm at one moment for one set of data and not for other sets of data is clearly taking a specific action based on the result of the filtering in the previous step.

As per claim 2:

Applicant asserts McCreery does not disclose a timeline in conjunction with the stated Official Notice. The Examiner points to Figure 5b-1/2 of McCreery showing a chronologically ordered (column labeled 563) and sequentially ordered (column 555) set of data. McCreery clearly shows the need for expressing data chronologically. Applicant additionally never challenged the Official Notice regarding the practice of presenting a timeline or the reasoning behind the combination of McCreery being obvious.

As per claim 4:

Applicant alleges there is not an agent present. McCreery discloses a packet analyzer as part of a larger system (column 4, lines 35-63). The term agent is given a reasonably broad interpretation on being something that acts as part of a system. As such, the packet analyzer satisfies the requirements of an agent.

As per claim 5:

Applicant alleges hunting, placing and forwarding is not present in McCreery. McCreery discloses that the analysis system forwards the alarm to a remote station (column 6, lines 60 through column 7, lines 4). Thus the packet analyzer gather the hunted data and the remote system receives the alerts with as described (column 8, lines 1-9).

As per claim 6

Applicant alleges there is not an agent present. McCreery discloses a packet analyzer as part of a larger system (column 4, lines 35-63). The term agent is given a reasonably broad interpretation on being something that acts as part of a system. As such, the packet analyzer satisfies the requirements of an agent.

As per claim 16:

Applicant asserts McCreery does not disclose a criteria. The Examiner points out that McCreery uses a rules based system, that is, a criteria is established by a set of rules (column 5, lines 50).

Applicant asserts McCreery does not disclose an action. The Examiner points out that McCreery generates an alarm, which is an action (column 6, lines 60-67).

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,
Bryce P. Bonzo
Bryce P Bonzo
Examiner
Art Unit 2114

June 14, 2004

Conferees Robert Beausoliel RWB
Eddie Chan

LOWE HAUPTMAN GILMAN & BERNER, LLP
Suite 310
1700 Diagonal Road
Alexandria, VA 22314

ROBERT BEAUSOLIEL
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

EDDIE CHAN
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

SCOTT BADERMAN
PRIMARY EXAMINER